WE CLAIM:

1. A data manager comprising:

a computer having a processor, an interface coupled with said processor and a memory coupled with said processor and said interface;

a first logic stored in said memory and executable by said processor to receive first data via said interface from a first entity, said first data comprising a first substantially unique representation and a first score associated with said first substantially unique representation, said first substantially unique representation being representative of a first identification parameter of a first entity, said first substantially unique representation being operative to substantially obscure said first identification parameter and substantially prevent said first identification parameter from being determined from said first substantially unique representation; and

a second logic coupled with said first logic and stored in said memory and executable by said processor to store said first substantially unique representation and said first score in said memory.

2. The data manager of Claim 1, further comprising:

a third logic stored in said memory and executable by said processor to receive a query via said interface from a third entity, said query comprising a second substantially unique representation of a second identification parameter, said second substantially unique representation being operative to substantially obscure said second identification parameter and to substantially prevent said second identification parameter from being determined from said second substantially unique representation, wherein said second substantially unique representation will be equivalent to said first substantially unique representation if said first identification parameter is equivalent to said second identification parameter;

a fourth logic coupled with said third logic and stored in said memory and executable by said processor to compare said second substantially unique representation with said stored first substantially unique representation; and

a fifth logic coupled with said fourth logic and stored in said memory and executable by said processor to transmit said stored first score to said third entity in response to said query if said second substantially unique representation is equivalent to said stored first substantially unique representation.

3. The data manager of Claim 2, wherein said stored first score is indicative of a likelihood of fraud.

4. The data manager of Claim 2, wherein said stored first score is indicative of a likelihood of suspicious activity.

5. The data manager of Claim 2, wherein said first entity is different from said third entity and further wherein said first entity is substantially incapable of determining said second value and said third entity is substantially incapable of determining said first value.

6. The data manager of Claim 1, wherein said first substantially unique representation comprises a hash of said first value.

7. The data manager of Claim 1, wherein said first substantially unique representation comprises an encryption of said first value.

8. The data manager of Claim 1, wherein said first entity comprises an entity having knowledge of suspicious activity.

9. The data manager of Claim 1, wherein said first entity comprises an entity having knowledge of fraudulent activity.

10. The data manager of Claim 1, wherein:

said first logic is further operative to receive second data from a third entity regarding said second entity via said interface, said second data comprising a second substantially unique representation and a second score associated with said second substantially unique representation, said second substantially unique representation being representative of a second value of said at least one parameter, said second substantially unique representation being operative to substantially obscure said second value and substantially prevent said second value from being determined from said second substantially unique representation; and further;

wherein said second logic is further operative to compare said second substantially unique representation with said stored first substantially unique representation, wherein said second substantially unique representation will be equivalent to said first substantially unique representation if said first value is equivalent to said second value; and

wherein said second logic is further operative to combine said first score and said second score and store said combination according to said first substantially unique representation in said memory if said stored first substantially unique representation is equivalent to said second substantially unique representation; and further;

wherein said second logic is further operative to store said second substantially unique representation and said second score in said memory according to said second substantially unique representation if said stored first substantially unique representation is not equivalent to said second substantially unique representation.

11. The data manager of Claim 10, wherein said combination is stored in place of said first score.

12. The data manager of Claim 10, wherein said combination comprises a mathematical combination of said first and second scores.

13. The data manager of Claim 1, wherein said at least one parameter comprises at least one of name, billing address, home address, business address, shipping address, email address, Internet Protocol ("IP") address, telephone number, social security number, bank account number, drivers license number, passport number, and credit card number.

14. A method comprising:

receiving, by first logic stored in a memory of a computer, said computer further comprising a processor coupled with said memory and an interface coupled with said processor and said memory, said first logic being executable by said processor, first data via said interface from said first entity, said first data comprising a first substantially unique representation and a first score associated with said first substantially unique representation, said first substantially unique representation being representative of a first value of said at least one parameter, said first substantially unique representation being operative to substantially obscure said first value and substantially prevent said first value from being determined from said first substantially unique representation, said first score being indicative of a likelihood that said first value may be associated with a first fraudulent transaction; and

storing, by second logic coupled with said first logic and stored in said memory and executable by said processor, said first substantially unique representation and said first score in said memory according to said first substantially unique representation.

15. The method of Claim 14, further comprising:

receiving, by third logic stored in said memory and executable by said processor, a query via said interface from said third entity, said query comprising a second substantially unique representation of a second value of said at least one parameter of said subsequent transaction, said second substantially unique representation being operative to substantially obscure said second value and to substantially prevent said second value from being determined from said second substantially unique representation, wherein said second substantially unique representation will be equivalent to said first substantially unique representation if said first value is equivalent to said second value;

comparing, by fourth logic coupled with said third logic and stored in said memory and executable by said processor, said second substantially unique representation with said stored first substantially unique representation; and transmitting, by fifth logic coupled with said fourth logic and stored in said memory and executable by said processor, said stored first score to said third entity in response to said query if said second substantially unique representation is equivalent to said stored first substantially unique representation;

wherein said computer is unaware of said second value.

16. The method of Claim 15, wherein said stored first score is indicative of a likelihood of fraud in said subsequent transaction.

17. The method of Claim 15, wherein said stored first score is indicative of a likelihood of suspicious activity in said subsequent transaction.

18. The method of Claim 15, wherein said first entity is different from said third entity and further wherein said first entity is substantially incapable of determining said second value and said third entity is substantially incapable of determining said first value.

19. The method of Claim 14, wherein said first substantially unique representation comprises a hash of said first value.

20. The method of Claim 14, wherein said first substantially unique representation comprises an encryption of said first value.

21. The method of Claim 14, wherein said first entity comprises an entity having knowledge of fraudulent activity.

22. The method of Claim 14, wherein:

receiving, by said first logic, second data from a third entity regarding said second entity via said interface, said second data comprising a second substantially unique representation and a second score associated with said second substantially unique representation, said second substantially unique representation being representative of a second value of said at least one parameter, said second substantially unique representation being operative to substantially obscure said second value and substantially prevent said second value from being determined from said second substantially unique representation, said second score being indicative of a likelihood that said second value may be associated with a second fraudulent transaction; and further;

comparing, by said second logic, said second substantially unique representation with said stored first substantially unique representation, wherein said second substantially unique representation will be equivalent to said first substantially unique representation if said first value is equivalent to said second value; and

combining, by said second logic, said first score and said second score and storing said combination according to said first substantially unique representation in said memory if said stored first substantially unique representation is equivalent to said second substantially unique representation; and further;

storing, by said second logic, said second substantially unique representation and said second score in said memory according to said second substantially unique representation if said stored first substantially unique representation is not equivalent to said second substantially unique representation.

23. The method of Claim 22, wherein said combining further comprises storing said combination in place of said first score.

24. The method of Claim 22, wherein said combining further comprises mathematically combining said first and second scores.

25. The method of Claim 14, wherein said at least one parameter comprises at least one of name, billing address, home address, business address, shipping address, email address, Internet Protocol ("IP") address, telephone number, social security number, bank account number, drivers license number, passport number, and credit card number.

26. A data manager for collecting information from a first entity regarding a second entity and disseminating said information to a third entity, said second entity being characterized by at least one parameter, said data manager further comprising:

a computer means having a processing means, an interface means coupled with said processing means and a memory means coupled with said processing means and said interface means;

first logic means, stored in said memory means and executable by said processing means, for receiving first data via said interface from said first entity, said first data comprising a first substantially unique representation and a first score associated with said first substantially unique representation, said first substantially unique representation being representative of a first value of said at least one parameter, said first substantially unique representation being operative to substantially obscure said first value and substantially prevent said first value from being determined from said first substantially unique representation, said first score being indicative of a likelihood that said first value may be associated with a first fraudulent transaction; and

second logic means coupled with said first logic means and stored in said memory means and executable by said processing means, for storing said first substantially unique representation and said first score in said memory according to said first substantially unique representation;

wherein said data manager is unaware of said first value.

27. The data manager of Claim 26, further comprising:

third logic means stored in said memory means and executable by said processing means, for receiving a query via said interface from said third entity, said query comprising a second substantially unique representation of a second value of said at least one parameter of said subsequent transaction, said second substantially unique representation being operative to substantially obscure said second value and to substantially prevent said second value from being determined from said second substantially unique representation, wherein said second substantially unique representation will be equivalent to said first substantially unique representation if said first value is equivalent to said second value;

fourth logic means coupled with said third logic means and stored in said memory means and executable by said processing means, for comparing said second substantially unique representation with said stored first substantially unique representation; and

fifth logic means coupled with said fourth logic means and stored in said memory means and executable by said processing means, for transmitting said stored first score to said third entity in response to said query if said second substantially unique representation is equivalent to said stored first substantially unique representation;

wherein said data manager is unaware of said second value.

28. The data manager of Claim 27, wherein said stored first score is indicative of a likelihood of fraud in said subsequent transaction.

29. The data manager of Claim 27, wherein said stored first score is indicative of a likelihood of suspicious activity in said subsequent transaction.

30. The data manager of Claim 26, wherein said first substantially unique representation comprises a hash of said first value.

31. The data manager of Claim 26, wherein said first substantially unique representation comprises an encryption of said first value.

32. The data manager of Claim 26, wherein:

said first logic means is further operative to receive second data from a third entity regarding said second entity via said interface, said second data comprising a second substantially unique representation and a second score associated with said second substantially unique representation, said second substantially unique representation being representative of a second value of said at least one parameter, said second substantially unique representation being operative to substantially obscure said second value and substantially prevent said second value from being determined from said second substantially unique representation, said second score being indicative of a likelihood that said second value may be associated with a second fraudulent transaction; and further;

wherein said second logic means is further operative to compare said second substantially unique representation with said stored first substantially unique representation, wherein said second substantially unique representation will be equivalent to said first substantially unique representation if said first value is equivalent to said second value; and

wherein said second logic means is further operative to combine said first score and said second score and store said combination according to said first substantially unique representation in said memory if said stored first substantially unique representation is equivalent to said second substantially unique representation; and further;

wherein said second logic means is further operative to store said second substantially unique representation and said second score in said memory according to said second substantially unique representation if said stored first substantially unique representation is not equivalent to said second substantially unique representation.

33. The data manager of Claim 32, wherein said combination is stored in place of said first score.

34. The data manager of Claim 32, wherein said combination comprises a mathematical combination of said first and second scores.

35. A system for collecting information from a first entity regarding a second entity and disseminating said information to a third entity, said second entity being characterized by at least one parameter, said system comprising:

a data receiver operative to receive first data from said first entity, said first data comprising a first substantially unique representation and a first score associated with said first substantially unique representation, said first substantially unique representation being representative of a first value of said at least one parameter, said first substantially unique representation being operative to substantially obscure said first value and substantially prevent said first value from being determined from said first substantially unique representation;

a data storage coupled with said data receiver and operative to store said first substantially unique representation and said first score according to said first substantially unique representation;

wherein said system is unaware of said first value.

36. The system of Claim 35, further comprising:

a query receiver operative to receive a query via said interface from said third entity, said query comprising a second substantially unique representation of a second value of said at least one parameter of said subsequent transaction, said second substantially unique representation being operative to substantially obscure said second value and to substantially prevent said second value from being determined from said second substantially unique representation, wherein said second substantially unique representation will be equivalent to said first substantially unique representation if said first value is equivalent to said second value;

a comparator coupled with said query receiver and operative to compare said second substantially unique representation with said stored first substantially unique representation; and

a score transmitter coupled with said comparator and operative to transmit said stored first score to said third entity in response to said query if said second substantially unique representation is equivalent to said stored first substantially unique representation;

wherein said system is unaware of said second value.

37. A method of collecting information by a collecting entity from a first entity regarding a second entity and disseminating said information to a third entity, said second entity being characterized by at least one parameter, said method comprising:

receiving first data from said first entity, said first data comprising a first substantially unique representation and a first score associated with said first substantially unique representation, said first substantially unique representation being representative of a first value of said at least one parameter, said first substantially unique representation being operative to substantially obscure said first value and substantially prevent said first value from being determined from said first substantially unique representation, said first score being indicative of a likelihood that said first value may be associated with a first fraudulent transaction;

storing said first substantially unique representation and said first score according to said first substantially unique representation;

wherein said collecting entity is unaware of said first value.

38. The method of Claim 37, further comprising:

receiving a query via said interface from said third entity, said query comprising a second substantially unique representation of a second value of said at least one parameter of said subsequent transaction, said second substantially unique representation being operative to substantially obscure said second value and to substantially prevent said second value from being determined from said second substantially unique representation, wherein said second substantially unique representation will be equivalent to said first substantially unique representation if said first value is equivalent to said second value;

comparing said second substantially unique representation with said stored first substantially unique representation; and

transmitting said stored first score to said third entity in response to said query if said second substantially unique representation is equivalent to said stored first substantially unique representation;

wherein said collecting entity is unaware of said second value.

39. The method of Claim 38, wherein said stored first score is indicative of a likelihood of fraud in said subsequent transaction. Criminal / suspicious

40. The method of Claim 38, wherein said stored first score is indicative of a likelihood of suspicious activity in said subsequent transaction.

41. A system for collecting information from a first entity regarding a second entity and disseminating said information to a third entity regarding a subsequent transaction between said second entity and said third entity, said second entity being characterized by at least one parameter, said system comprising:

data receiving means for receiving first data from said first entity, said first data comprising a first substantially unique representation and a first score associated with said first substantially unique representation, said first substantially unique representation being representative of a first value of said at least one parameter, said first substantially unique representation being operative to substantially obscure said first value and substantially prevent said first value from being determined from said first substantially unique representation, said first score being indicative of a likelihood that said first value may be associated with a first fraudulent transaction;

data storage means, coupled with said data receiving means, for storing said first substantially unique representation and said first score according to said first substantially unique representation;

wherein said system is unaware of said first value.

42. The system of Claim 41, further comprising:

query receiving means for receiving a query via said interface from said third entity, said query comprising a second substantially unique representation of a second value of said at least one parameter of said subsequent transaction, said second substantially unique representation being operative to substantially obscure said second value and to substantially prevent said second value from being determined from said second substantially unique representation, wherein said second substantially unique representation will be equivalent to said first substantially unique representation if said first value is equivalent to said second value;

comparator means, coupled with said query receiver, for comparing said second substantially unique representation with said stored first substantially unique representation; and score transmitter means, coupled with said comparator, for transmitting said stored first score to said third entity in response to said query if said second substantially unique representation is equivalent to said stored first substantially unique representation;

wherein said system is unaware of said second value.

43. A transaction manager for communicating information regarding a first entity, said information being further related to a first transaction involving said first entity, said first entity being characterized by at least one parameter, said system comprising:

a computer having a processor, an interface coupled with said processor and a memory coupled with said interface and said processor;

first logic stored in said memory and executable by said processor, said first logic being operative to determine whether said first transaction is one of pending and complete;

second logic, coupled with said first logic, stored in said memory and executable by said processor, and operative, if said first transaction is pending, to determine a value of said at least one parameter and generate a first substantially unique representation of said value, said first substantially unique representation being operative to substantially obscure said value and substantially prevent said value from being determined from said first substantially unique representation;

third logic, coupled with said second logic, stored in said memory and executable by said processor, and operative to transmit said first substantially unique representation via said interface to a transaction processor and receive a subsequent response therefrom; and

fourth logic, coupled with said first logic, stored in said memory and executable by said processor, and operative, if said first transaction is complete, to determine whether said first transaction is fraudulent, said fourth logic being further operative, if said first transaction is determined to be fraudulent, to compute a second score, based on said first transaction, indicative of the likelihood that a subsequent transaction with said first entity will be fraudulent and to further determine a value of said at least one parameter and generate a second substantially unique representation of said value, said second substantially unique representation being operative to substantially obscure said value and substantially prevent said value from being determined from said second substantially unique representation, wherein said fourth logic is further operative to communicate said second score and said second substantially unique representation to said transaction processor via said interface.

44. The transaction manager of Claim 43, further comprising:

fifth logic, coupled with said third logic, stored in said memory and executable by said processor, and operative to one of approve, disapprove and modify said first transaction based on said first score.

45. The transaction manager of Claim 43, wherein said second and fourth logic further comprise a hash function operative to generate said first and second substantially unique representations as hashes of said first and second values, respectively.

46. A method implemented in a computer for communicating information regarding a first entity, said information being further related to a first transaction involving said first entity, said first entity being characterized by at least one parameter, said method comprising:

determining, by first logic stored in a memory of a computer, said computer further comprising a processor coupled with said memory and an interface coupled with said processor and said memory, said first logic being executable by said processor, whether said first transaction is one of pending and complete;

determining, by second logic, coupled with said first logic, stored in said memory and executable by said processor, if said first transaction is pending, a value of said at least one parameter and generating a first substantially unique representation of said value, said first substantially unique representation being operative to substantially obscure said value and substantially prevent said value from being determined from said first substantially unique representation;

transmitting, by third logic, coupled with said second logic, stored in said memory and executable by said processor, said first substantially unique representation via said interface to a transaction processor and receiving a subsequent response therefrom; and

determining, by fourth logic, coupled with said first logic, stored in said memory and executable by said processor, if said first transaction is complete, whether said first transaction is fraudulent, and, if said first transaction is determined to be fraudulent, computing a second score, based on said first transaction, indicative of the likelihood that a subsequent transaction with said first entity will be fraudulent, determining a value of said at least one parameter and generating a second substantially unique representation of said value, said second substantially unique representation being operative to substantially obscure said value and substantially prevent said value from being determined from said second substantially unique representation, and communicating said second score and said second substantially unique representation to said transaction processor via said interface.

9

47. A method for communicating non-secure data between a first entity and a second entity, said first and second entities each having access to secure data, said method comprising:

acquiring said non-secure data, said non-secure data requiring said secure data to substantially contextualize said non-secure data;

generating a substantially unique representation of said secure data, said substantially unique representation being operative to substantially obscure said secure data and substantially prevent said secure data from being determined from said substantially unique representation; and

transmitting said non-secure data and said substantially unique representation to said second entity.

10

48. A method for communicating non-secure data between a first entity and a second entity, said first entity having access to first secure data and said second entity

having access to second secure data, said method comprising:

receiving said non-secure data from said first entity, said non-secure data requiring said secure data to substantially contextualize said non-secure data;

receiving a first substantially unique representation of said first secure data from said first entity, said first substantially unique representation being operative to substantially obscure said first secure data and substantially prevent said first secure data from being determined from said first substantially unique representation;

generating a second substantially unique representation of said second secure data, said second substantially unique representation being operative to substantially obscure said second secure data and substantially prevent said second secure data from being determined from said second substantially unique representation;

comparing said first and second substantially unique representations;

using said second secure data, where said first substantially unique representation is equivalent to said second substantially unique representation, to contextualize said non-secure data.